Stand-Alone Firewalls - External Preventive Measures

David Tran - A00801942 | Cole Rees - A00741578

COMP 6D

COMP 8006 - Assignment 2

British Columbia Institute of Technology

Aman Abdulla

Thursday, February 20 2014

Table of Contents

# Background

The purpose of this assignment is to further the understanding of firewalls for the budding administrator. We will be implementing a standalone firewall that will be located externally of our internal host. This will allow us to have some control over what goes to and from our host through our external firewall host. For further information of our system and setup procedures, please refer to the **Design & Testing** document located on-disk.

# Tools & Equipment

## Hardware

|  |  |  |
| --- | --- | --- |
| * 8GB RAM | * Intel i5 Quad Core | * 500GB HDD |
| * em1 & p3p1 network cards | * firewall host | * internal host |
| * tertiary host for testing | * CAT5 Ethernet Cable |  |

## Software

|  |  |  |
| --- | --- | --- |
| * Fedora Linux 19 64-bit | * hping3 | * Shell Scripting |
| * Wireshark | * iptables |  |

# Testing Procedure

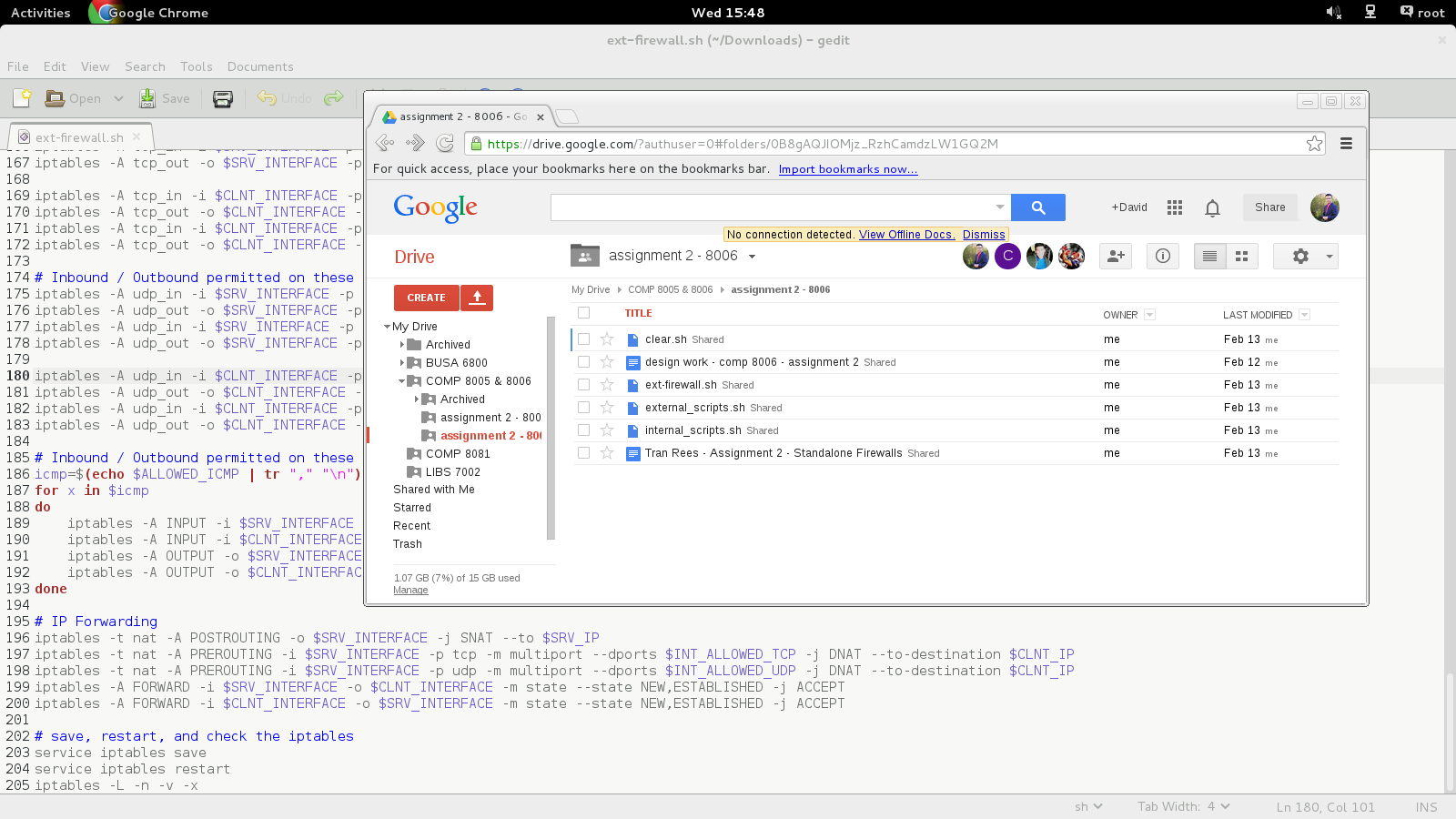
## Test Cases Table

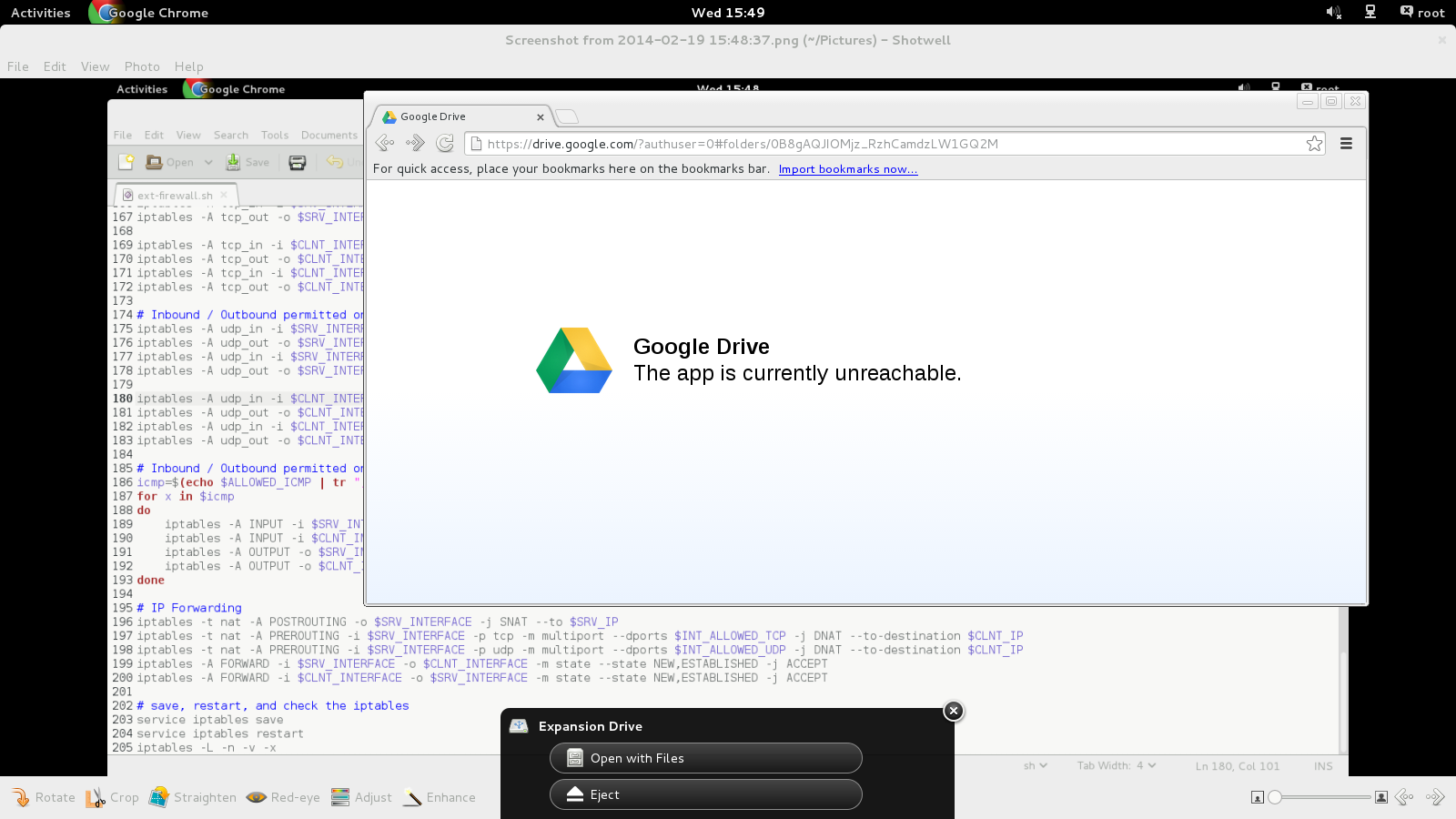
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Case #** | **Test Case** | **Tools Used** | **Expected Outcome** | **Results** |
| 1 | Firewall host has no external access | Google Chrome | Limited responses from the external network, no internet access | PASSED. See results. |
| 2 | Internal host has external access | Wireshark, Google Chrome | Can access internet, can receive external responses | PASSED. See results. |
| 3 | In / Out TCP permitted on specified ports | internal\_scripts.sh,  hping3 | Specified ports are permitted | PASSED.  See results. |
| 4 | In / Out TCP permitted on specified ports | internal\_scripts.sh, hping3 | Unspecified ports dropped. | PASSED. |
| 5 | In / Out UDP permitted on specified ports | internal\_scripts.sh,  hping3 | Specified ports are permitted | PASSED. See results. |
| 6 | In / Out UDP permitted on specified ports | internal\_scripts.sh,  hping3 | Other ports are dropped | PASSED. See results. |
| 7 | In / Out ICMP permitted on specified type numbers | internal\_scripts.sh, ping,  hping3 | Ping is allowed. | PASSED.  See results. |
| 8 | In / Out ICMP permitted on specified type numbers | external\_scripts.sh,  hping3 | Other icmp types are dropped. | PASSED.  See results. |
| 9 | All packets that fall through to the default rule will be dropped | external\_scripts.sh,  hping3 | Default policies are DROP; expected packet drops | PASSED. See results. |
| 10 | All packets targeting the firewall host (externally) will be dropped | external\_scripts.sh,  hping3 | Packets are expected to be dropped | PASSED. See results. |
| 11 | Drop all packets from hosts pretending to be an internal host | external\_scripts.sh,  hping3 | Drop those packets from the external network | PASSED. See results. |
| 12 | Drop all packets from hosts pretending to be an internal host | internal\_scripts.sh,  hping3 | Accept packets from the internal network | PASSED. See results. |
| 13 | Reject all inbound SYN packets (with targets to “high” ports) | external\_scripts.sh,,  hping3 | Packets will be dropped (no target) | PASSED. See results. |
| 14 | Reject all inbound SYN packets (with targets to “high” ports) | external\_scripts.sh,,  hping3 | Packets will be dropped (with targets) | PASSED. See results. |
| 15 | Accept all incoming fragments | external\_scripts.sh,,  hping3 | All following fragments, if the first fragment is accepted, will be accepted | PASSED. See results. |
| 16 | Accept all incoming fragments | external\_scripts.sh,,  hping3 | All following fragments, if the first fragment is dropped, will be dropped | PASSED. See results. |
| 17 | Accept all TCP packets that belong to an existing connection (on allowed ports) | external\_scripts.sh,,  hping3 | Check if the state is “ESTABLISHED”; if it is, accept. | PASSED. See results. |
| 18 | Accept all TCP packets that belong to an existing connection (on allowed ports)  (non syn packet) | external\_scripts.sh,,  hping3 | Check if the state is “Established”; if it is “NEW”, drop. | PASSED. See results. |
| 19 | Drop all packets with the SYN and FIN bits set | external\_scripts.sh,,  hping3 | Check if the SYN bit is flagged. If it is and state is NEW, drop it. | PASSED. See results. |
| 20 | Drop all packets with the SYN and FIN bits set | external\_scripts.sh,,  hping3 | Check if the FIN bit is flagged. If it is and state is NEW, drop it. | PASSED. See results. |
| 21 | Drop all packets with the SYN and FIN bits set | external\_scripts.sh,  hping3 | Check if the SYN and FIN bit are flagged. If it is and state is NEW, drop it. | PASSED. See results. |
| 22 | Drop all Telnet packets | external\_scripts.sh,  hping3 | Incoming Telnet packets are dropped (internal) | PASSED. See results. |
| 23 | Drop all Telnet packets | internal\_scripts.sh,  hping3 | Incoming Telnet packets are dropped (external) | PASSED. See results. |
| 24 | Drop all Telnet packets | external\_scripts.sh,  hping3 | Outgoing Telnet packets are dropped (internal) | PASSED. See results. |
| 25 | Block all external traffic directed to ports 32768-32775, 137-139 and TCP ports 111 and 515 | external\_scripts.sh,  hping3 | Target host will be firewall; drop all packets | PASSED. See results. |
| 26 | Block all external traffic directed to ports 32768-32775, 137-139 and TCP ports 111 and 515 | internal\_scripts.sh,  hping3 | From internal host, target is firewall; still drop | PASSED. See results. |
| 27 | Set control connections to Minimum Delay for SSH and FTP applications | external\_scripts.sh,  hping3,  iptables,  Wireshark | Applications are set to “Minimum Delay” and tables reflect settings | PASSED. See results. |
| 28 | Set control connections to Minimum Delay for SSH and FTP applications | external\_scripts.sh,  hping3,  iptables,  Wireshark | Applications are set to “Minimum Delay” and tables reflect settings | PASSED. See results. |
| 29 | Set control connections to Maximum Throughput for FTP | external\_scripts.sh,  iptables,  Wireshark | Application is set to “Maximum Throughput” for FTP-data and tables reflect settings | PASSED. See results. |

## Test Case Evidence & Details

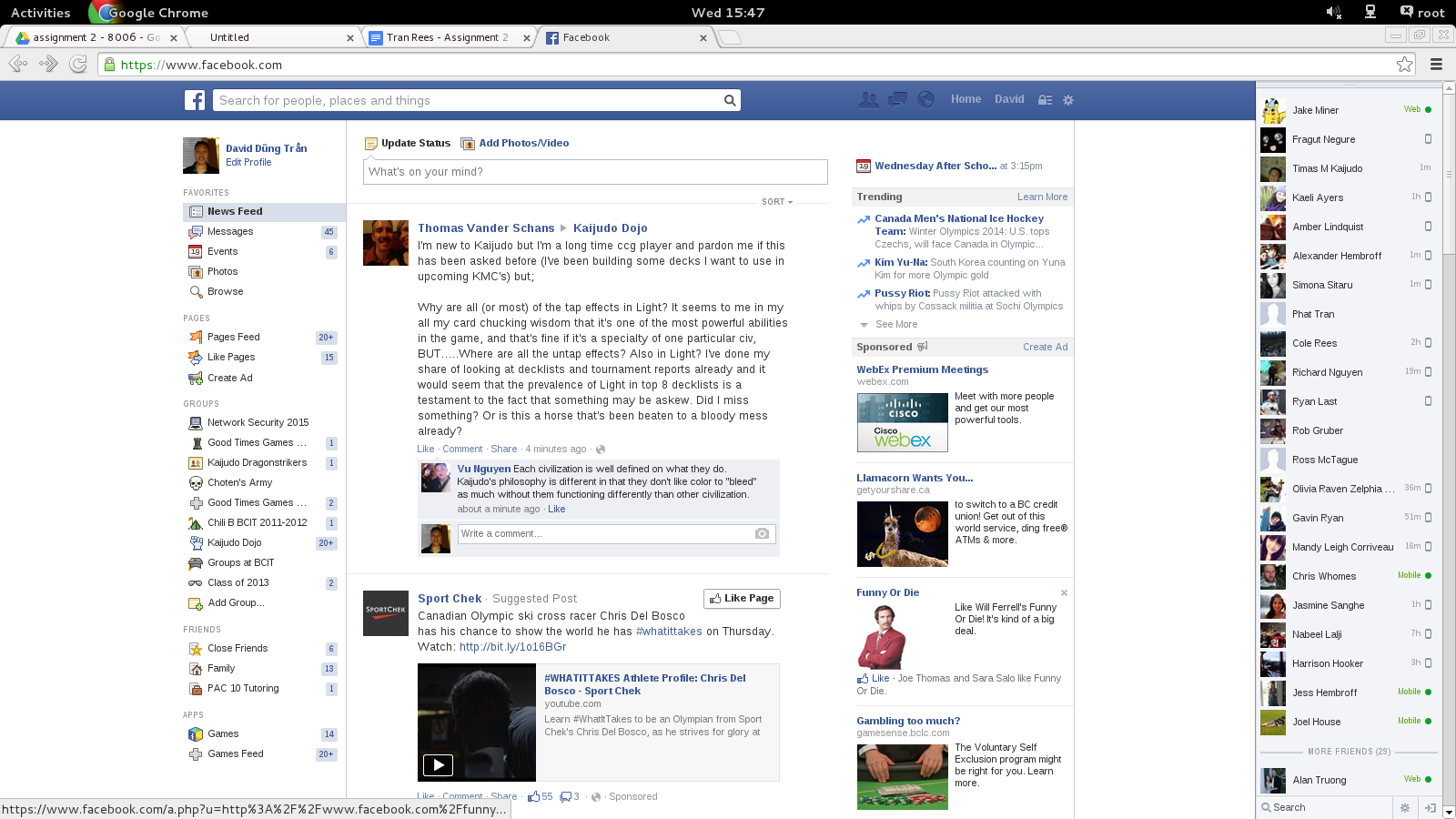
(1) Firewall has no external access

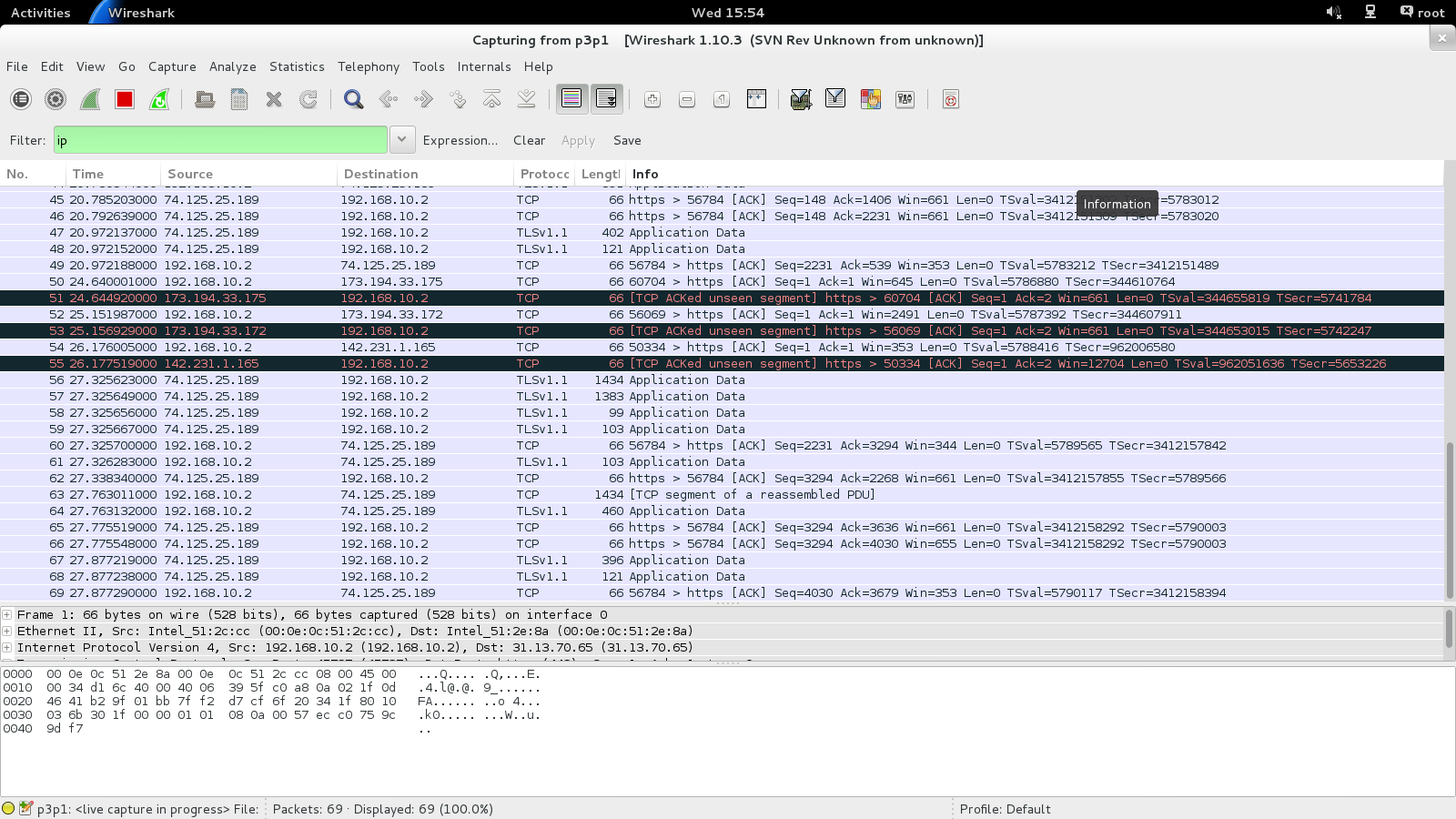
On the Firewall host, we opened Google Chrome browser, and saw no connections. This is prior to the Firewall rules were imposed. Note the “No connection from Google Drive.”

Then we refreshed the page. This is our result, which is expected:



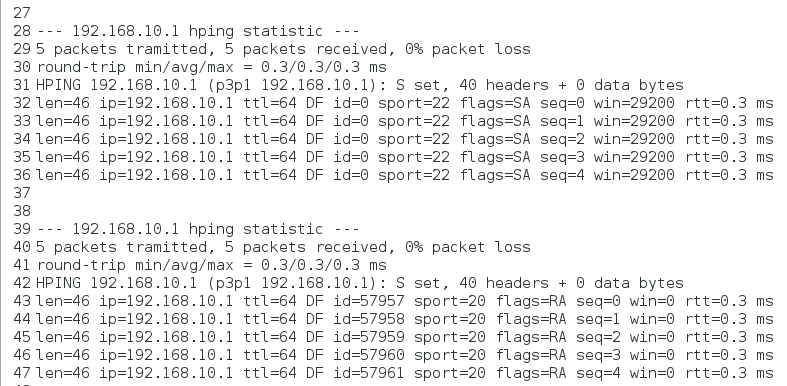
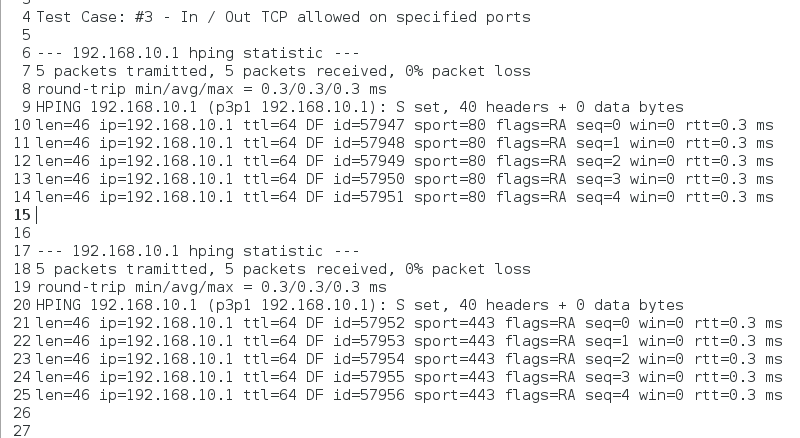
(2) This is a screenshot of the internal host after Firewall rules have been imposed externally.

And a Wireshark capture:

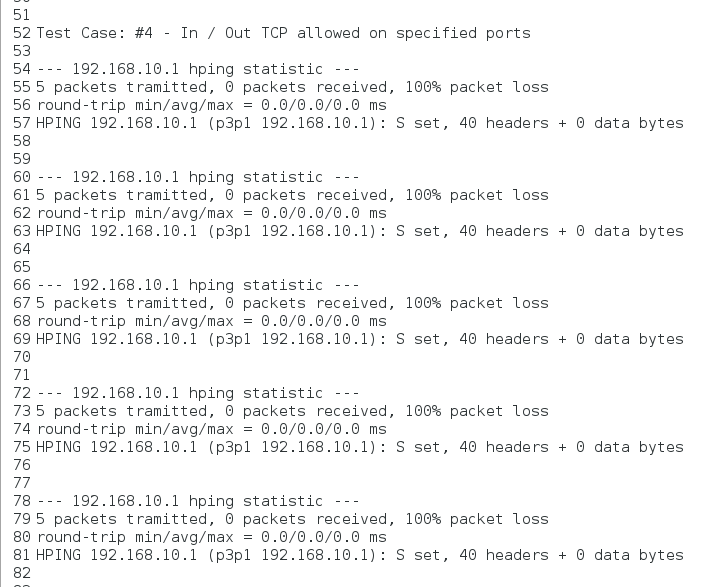


(3) Inbound and Outbound permissible TCP

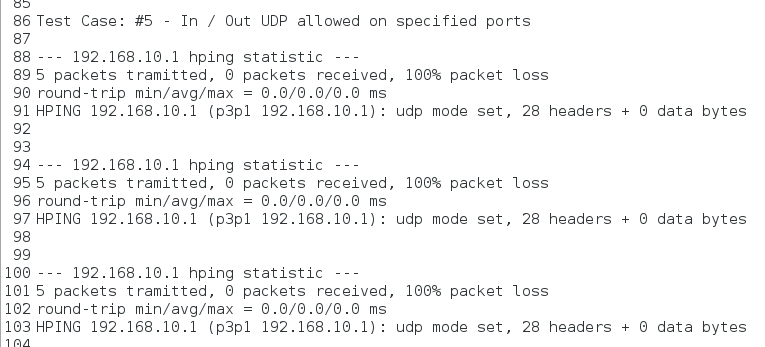
Here are the results of our test cases in our external text document generated from internal\_scripts.sh:

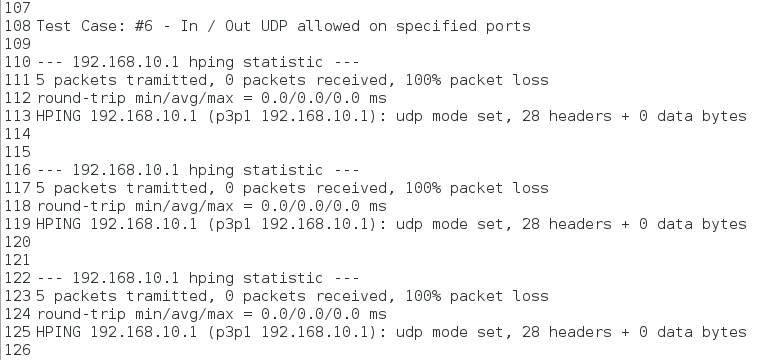


(4) Not permissible TCP traffic

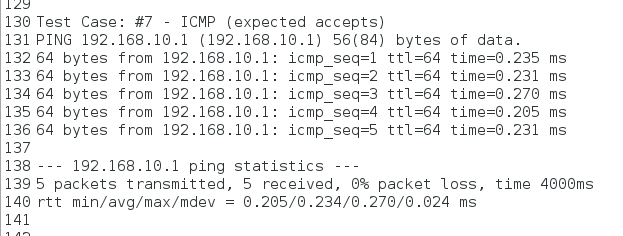


(5) and (6) Permissible and Non-Permissible UDP Packets:

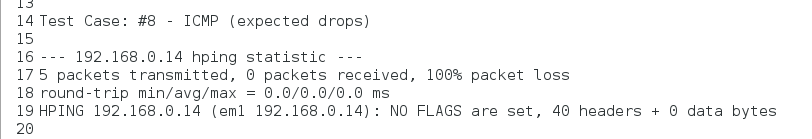
Note the dropped packets in Test Case 5. We suspect that Hping3 is creating malformed packets. We will assume that proper UDP packets will pass through.

Here, the drops are expected.

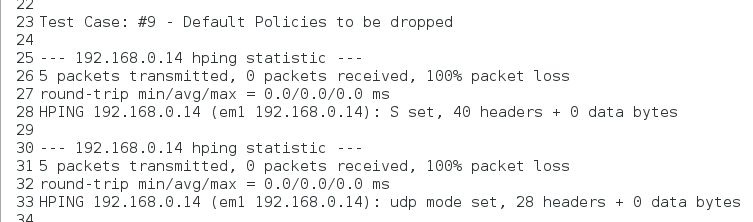
(7) Accepted ICMP

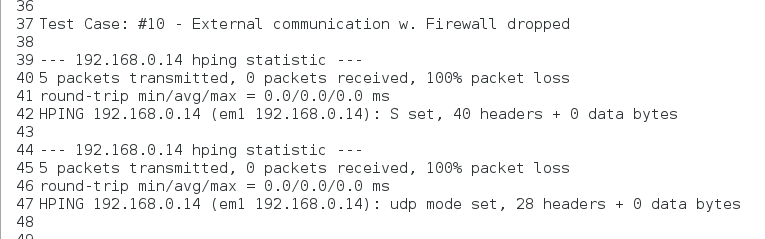


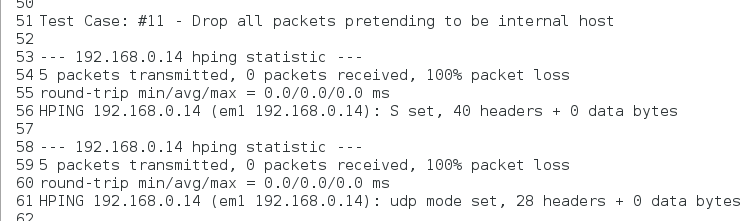
(8) Expected ICMP drops

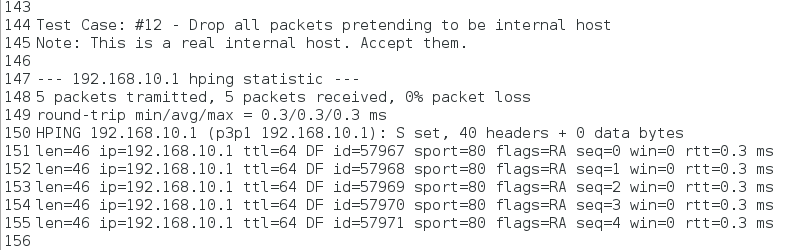


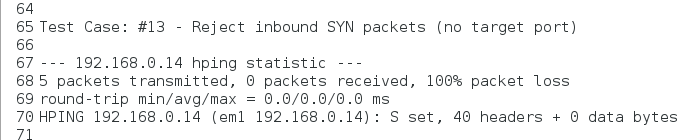
(9) Default policies to be dropped

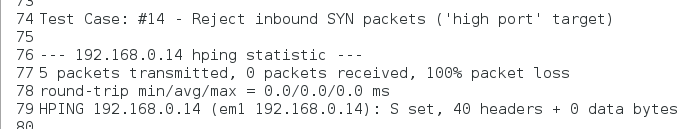


(10) External communication with the Firewall Host to be dropped (11) Stop all packets from fake hosts

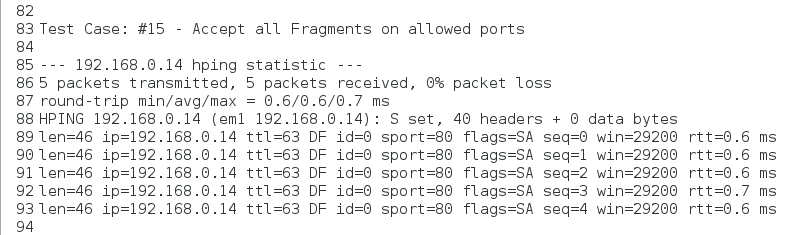


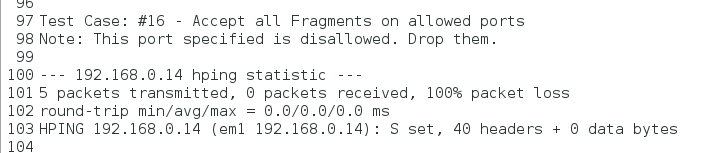
(12) This is an actual internal host. Allow these packets. 

(13) Reject inbound SYN packets to random ports 

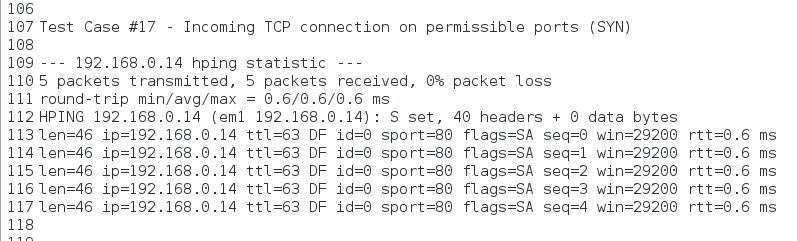
(14) Reject inbound SYN packets to “high” ports 

(15) Accept all fragments on allowed ports

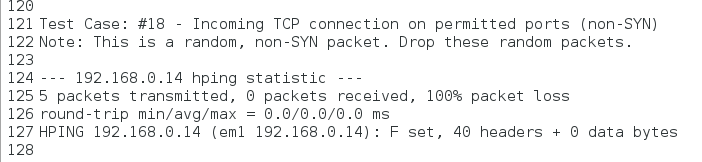


(16) Fragments on bad ports. Drop them. 

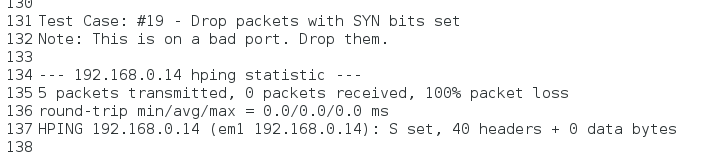
(17)



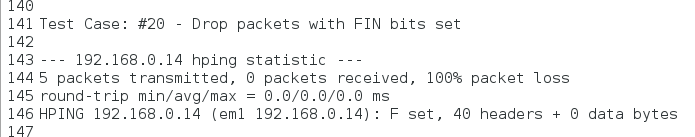
(18)



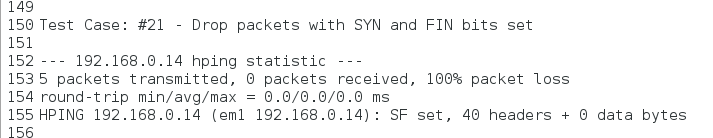
(19)



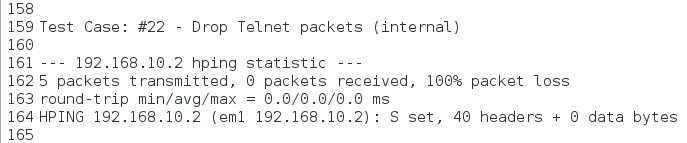
(20)



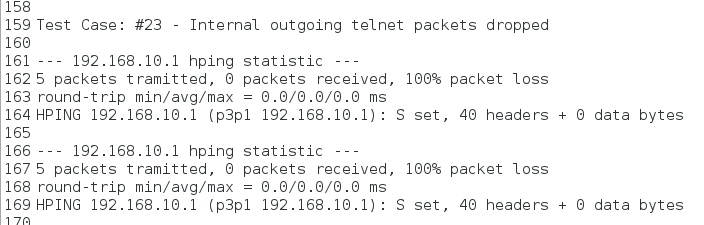
(21)



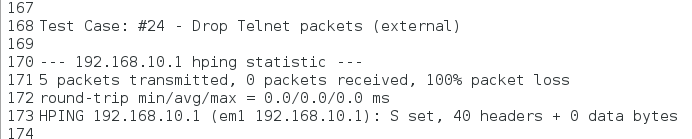
(22)



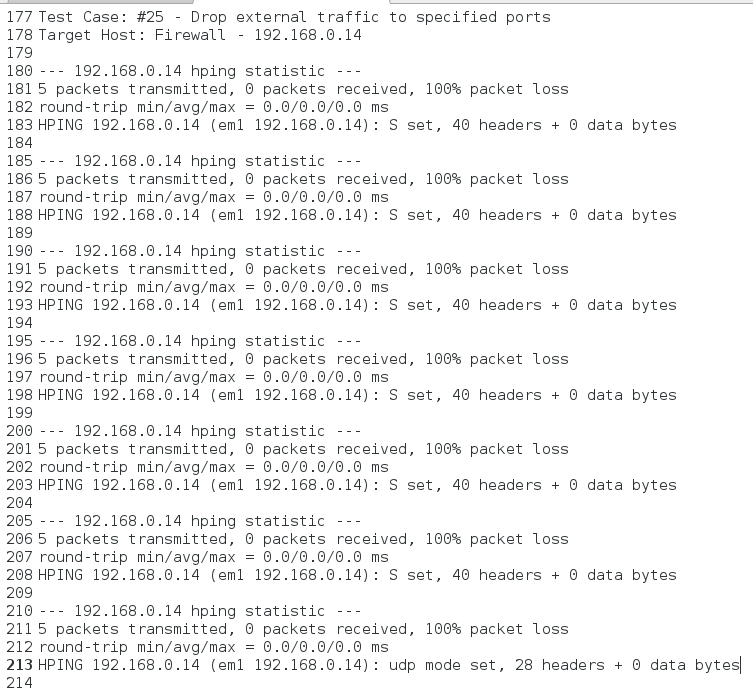
(23)

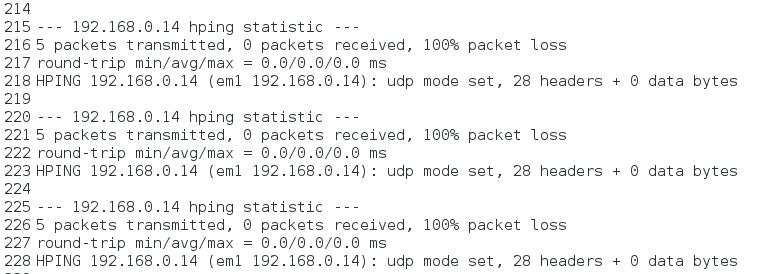


(24)

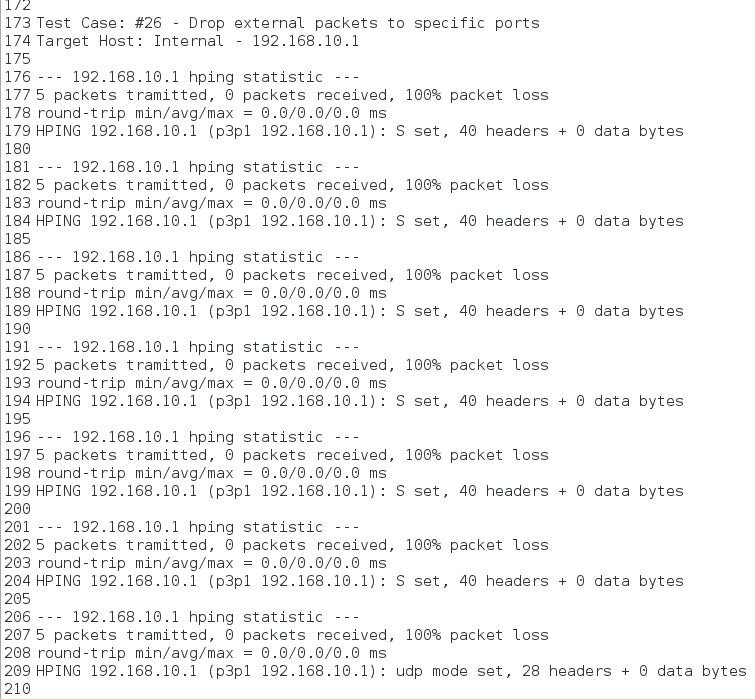


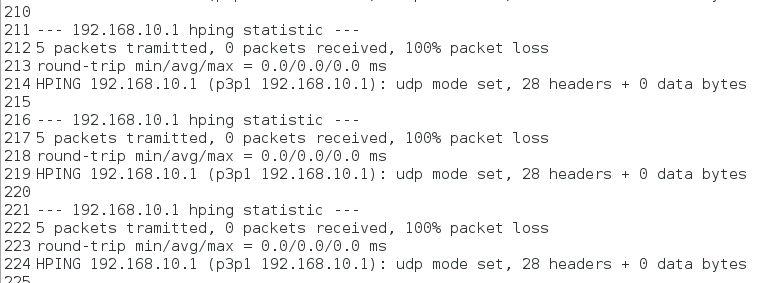
(25)



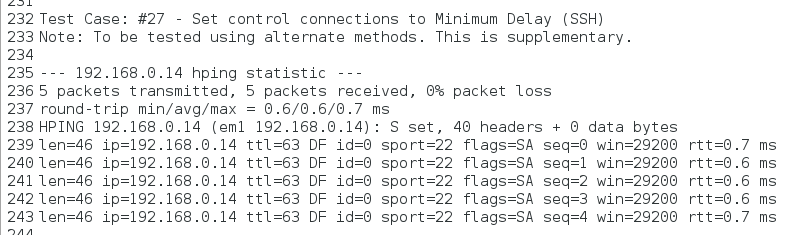


(26)

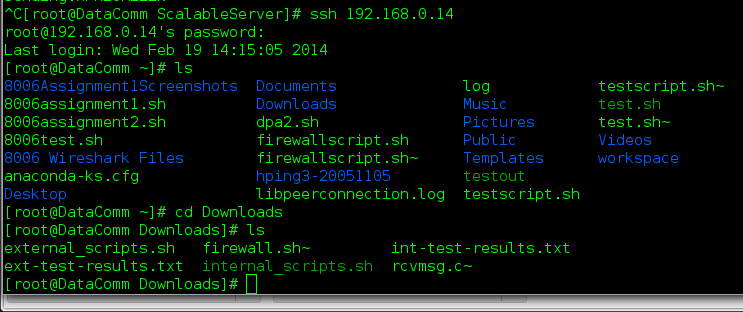




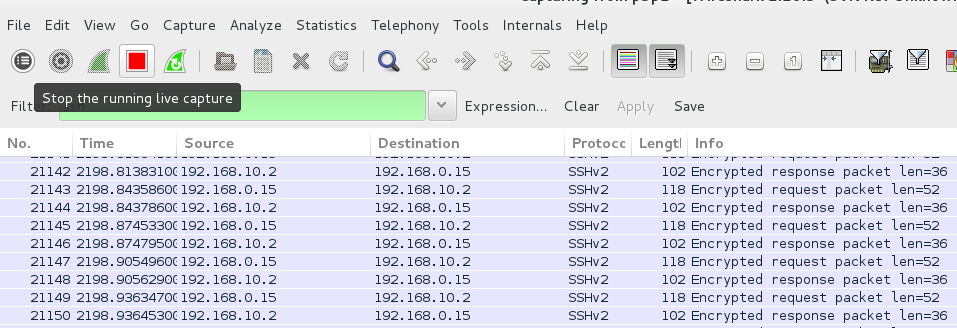
(27) Control connections for SSH to Minimum Delay. To do this, we will have a tertiary host ssh into our internal machine. Below is to show that ssh is allowed through the firewall.



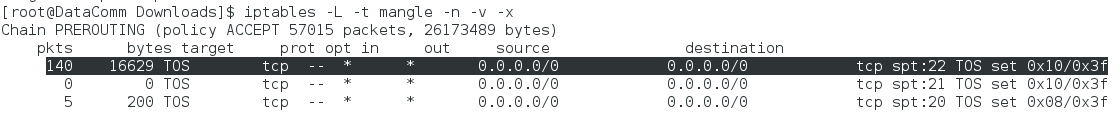
Now we ssh into the internal host:



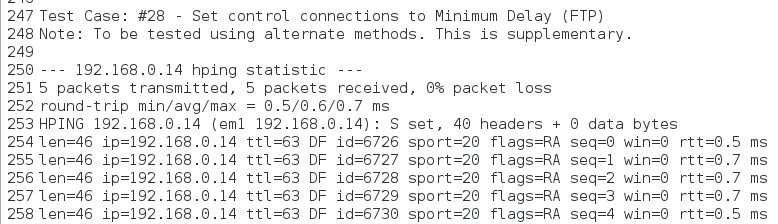
Our Wireshark capture:



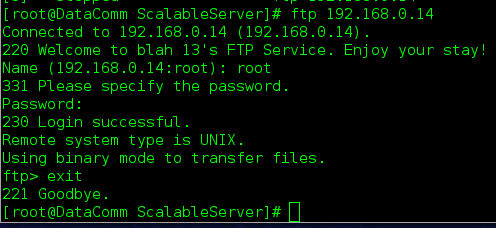
And our mangle table:



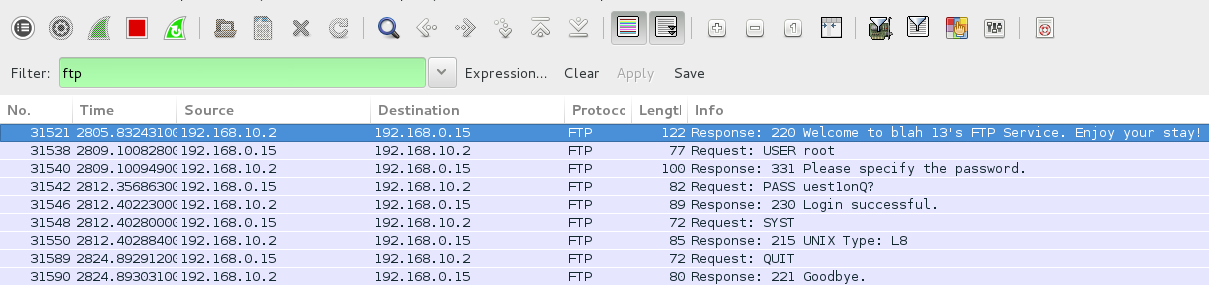
(28) Control connections for FTP to Minimum Delay. To do this, we will have a tertiary host ssh into our internal machine. Below is to show that ftp is allowed through the firewall.



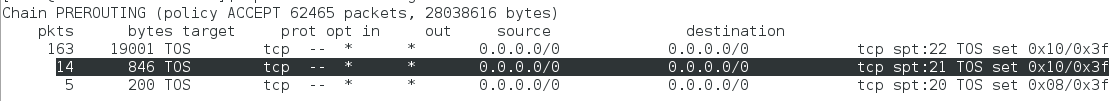
Because our internal host has ftp-server capabilities (see **Design & Testing** document), we will be able to access ftp capabilities externally:



Our Wireshark capture:

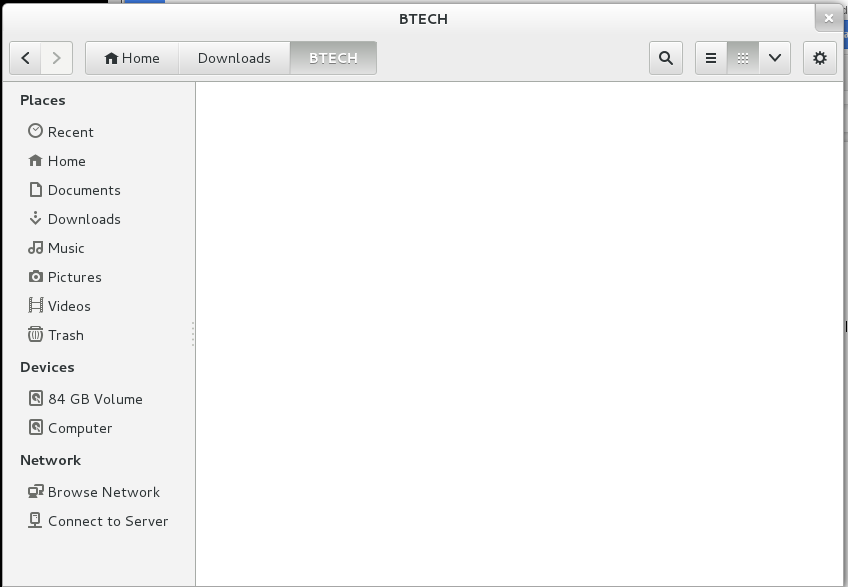


And our mangle table:

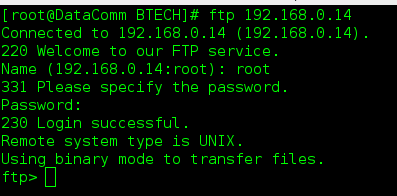


(29) FTP-data with Maximum-Throughput

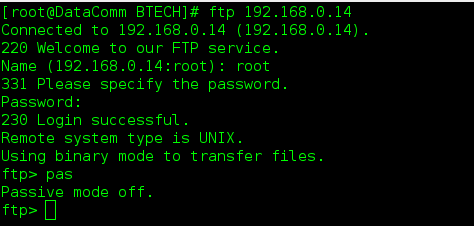
We would want to reconnect to our server. We’ll navigate to an arbitrary folder. For this example, our directory is /root/Downloads/BTECH. For proof, here’s its emptiness:



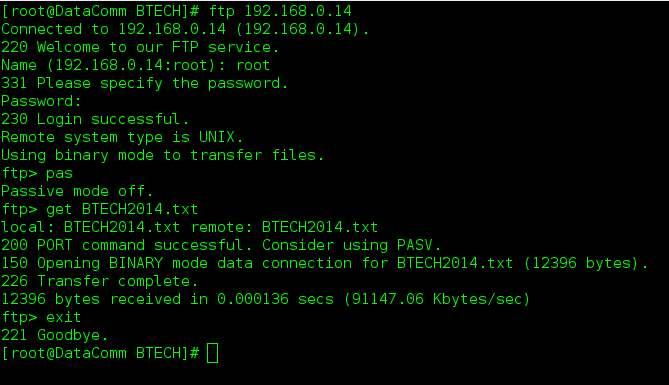
Let’s FTP into our host again:



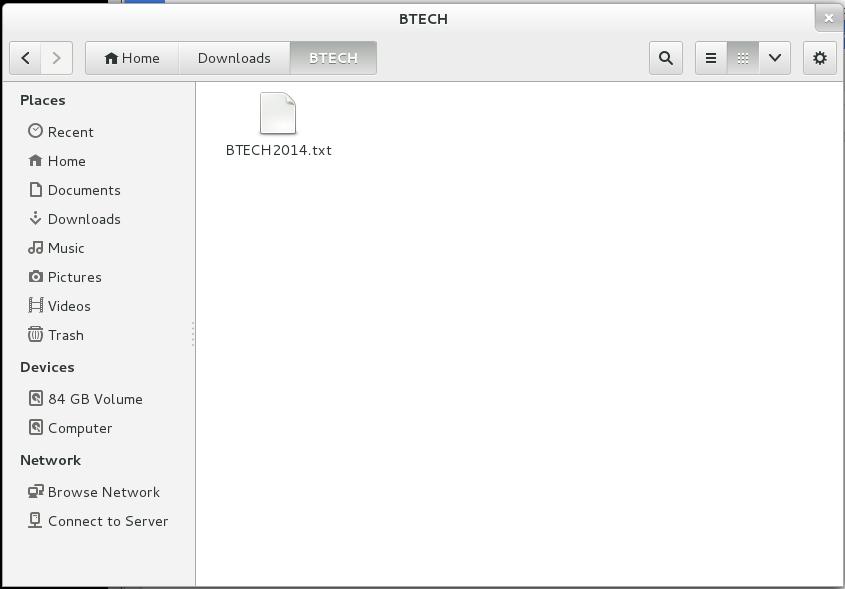
At this point, we should turn off Passive Mode, for the sake of easiness:



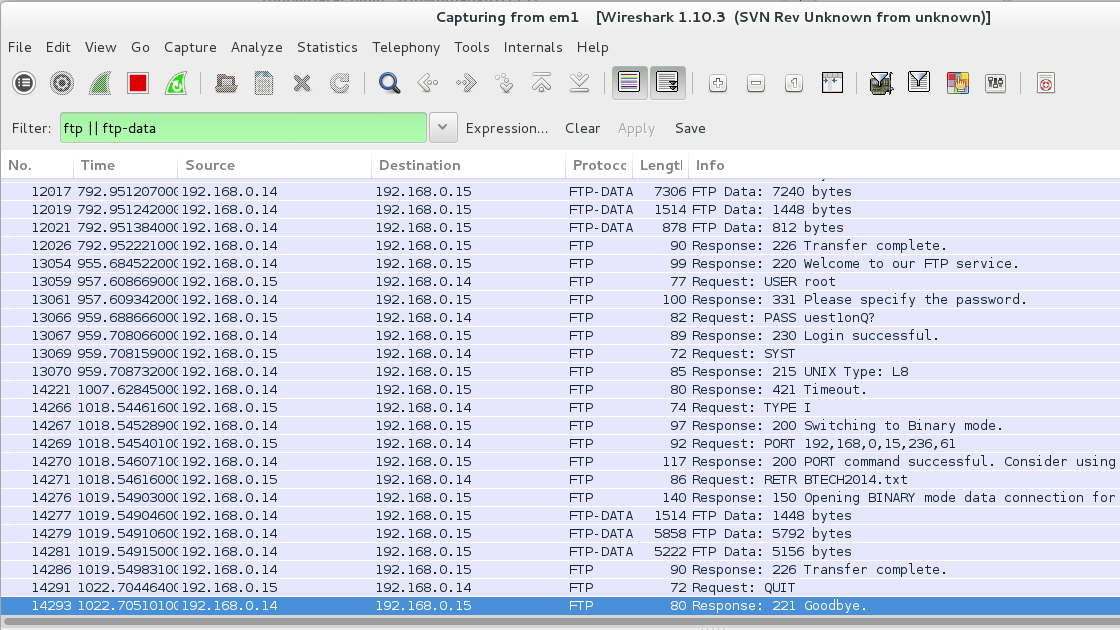
Now, let’s fetch some random data:



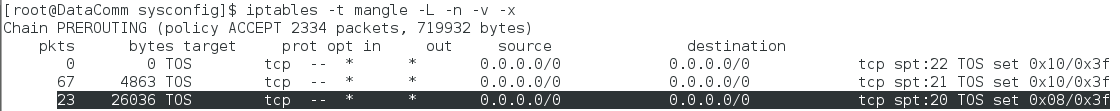
Check our local (external) directory:



Some external Wireshark capture:



Finally, our mangle table:



# Conclusion

Upon finishing this report of Assignment 2, we conclude that our Firewall implementation matches the following criteria:

On the OS level:

* Set the default policies (to drop)
* Inbound/Outbound TCP packets on allowed ports.
* Inbound/Outbound UDP packets on allowed ports.
* Inbound/Outbound ICMP packets based on type numbers.
* All packets that fall through to the default rule will be dropped.
* Drop all packets destined for the firewall host from the outside.
* Do not accept any packets with a source address from the outside matching your internal network.
* You must ensure the you reject those connections that are coming the “wrong” way
* Accept fragments.
* Accept all TCP packets that belong to an existing connection (on allowed ports).
* Drop all TCP packets with the SYN and FIN bit set.
* Do not allow Telnet packets at all.
* Block all external traffic directed to ports 32768 – 32775, 137 – 139, TCP ports 111 and 515.
* For FTP and SSH services, set control connections to "Minimum Delay" and FTP data to "Maximum Throughput".

On the scripting level:

* A user-configuration section which includes:
  + Name and location of the utility you are using to implement the firewall.
  + Internal network address space and the network device.
  + Outside address space and the network device.
  + TCP services that will be allowed.
  + UDP services that will be allowed.
  + ICMP services that will be allowed
* A implementation section which includes all the firewall rules as stated above

On the Physical level:

* The machines in the lab are equipped with two Ethernet cards. One of them is already configured and operational. You will have to enable and configure the other one for use as the gateway to your “internal” network.
* Your testbed will then have one machine operating as a firewall. It will have an “outside” connection (eth0) and it will forward datagrams to hosts on its internal hosts on the second NIC (eth1).

After full implementation of all the criterions above, our internal host was converted into a server, where ssh, ftp and http were acknowledged and permitted. We saw external access was directed to the firewall host, and then the firewall host was forwarding all the safe and correct traffic towards our internal host.

This is the essence of demilitarized zones (DMZ) and is an introduction to stand-alone firewalls.

# 

# 

# Appendix

Located on disk are the following:

* Stand-Alone Firewalls - External Preventive Measures (.pdf)
* Stand-Alone Firewalls - Design Work & Testing (.pdf)
* ext-firewall.sh
* external\_scripts.sh
* internal\_scripts.sh
* ext-test-results.txt (product of external\_scripts.sh)
* int-test-results.txt (product of internal\_scripts.sh)
* custom vsftpd.conf
  + <https://github.com/curationexperts/hydradam/wiki/Sample-vsftpd.conf>
* BTECH2014.txt (lorem ipsum, for testing ftp)
* README.txt